INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-30 06:23 UTC

Attorney General Bonta Sues Chrome Holding Co., Formerly Known as 23andMe, Over 2023 Data Breach

DATA BREACH | HIGH | CVSS 7.5

SCC Item ID	SCC-DBR-2026-0144
Type	Data Breach
Severity	HIGH
CVSS Base Score	7.5
Affected Products	23andMe (Chrome Holding Co.), consumer genetic testing platform; approximately 855,000 California residents affected
Published	1 day ago
Discovery Source	Serper

Executive Summary

California Attorney General Rob Bonta has filed suit against Chrome Holding Co. (formerly 23andMe) over its 2023 data breach, which exposed sensitive genetic and personal data belonging to approximately 855,000 California residents. The breach originated from a credential stuffing attack that exploited the platform's DNA Relatives feature, enabling mass scraping of linked user profiles. The lawsuit alleges the company failed to implement basic security controls and properly notify affected users, creating significant regulatory and reputational liability for any organization that handles similarly sensitive biometric or genetic data.

Technical Analysis

The 2023 23andMe breach was executed via credential stuffing (T1110.004), using previously compromised username/password pairs to authenticate against legitimate user accounts (T1078). Once authenticated, attackers exploited the DNA Relatives feature to traverse and scrape profile data from millions of accounts connected to the initial set of compromised credentials (T1530, Data from Cloud Storage). The attack did not require a novel exploit; it succeeded because 23andMe lacked effective brute-force protections (CWE-307: Improper Restriction of Excessive Authentication Attempts), exposed sensitive genetic profile data through authenticated but insufficiently access-controlled social features (CWE-359: Exposure of Private Personal Information to an Unauthorized Actor), and had insecure default configurations (CWE-1188: Insecure Default Initialization of Resource). No CVE has been assigned. The company subsequently filed for bankruptcy in 2025

and now operates as Chrome Holding Co. Patch status is not applicable; this is an architectural and operational control failure, not a software vulnerability with a vendor-issued fix.

Action Checklist

1. Containment, Audit all consumer-facing applications that expose social or network-graph features (e.g., 'connected accounts', 'people you know', 'data sharing' toggles). Immediately evaluate whether an authenticated user can traverse beyond their own data to scrape peer profiles. Disable or rate-limit any such feature until access controls are verified.
2. Detection, Review authentication logs for high-volume login attempts against a single account or distributed low-volume attempts across many accounts (credential stuffing signature). In your SIEM, query for: multiple failed logins followed by success from the same IP or IP range; single accounts accessed from geographically anomalous locations in short windows; and abnormal API or feature call volumes on data-sharing or social-graph endpoints. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs).
3. Eradication, Enforce account lockout or CAPTCHA challenges after a defined number of failed login attempts per NIST AC-7 (Unsuccessful Logon Attempts). Require multi-factor authentication on all consumer accounts per CIS 6.3 (Require MFA for Externally-Exposed Applications). Apply least-privilege data access to social or network features so authenticated users can only retrieve their own records per NIST AC-6 (Least Privilege) and NIST AC-3 (Access Enforcement).
4. Recovery, After tightening controls, verify remediation by running a controlled credential stuffing simulation (low-volume, authorized) against your authentication endpoints to confirm lockout thresholds trigger correctly. Monitor for resumed anomalous login patterns for at least 30 days. Validate that the DNA Relatives-style traversal pattern (authenticated user accessing peer profile data at scale) is no longer possible per NIST AC-4 (Information Flow Enforcement).
5. Post-Incident, Conduct a formal review of data minimization and access control design for any feature that exposes user-to-user data relationships. Map findings to NIST AC-5 (Separation of Duties) and NIST AC-6 (Least Privilege). Review breach notification procedures against applicable state privacy laws. Document findings in your risk register and update your incident response playbook to include credential stuffing as an explicit scenario. Apply D3-MFA (Multi-factor Authentication) and D3-UAP (User Account Permissions) as standing countermeasures.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to legal counsel, the CISO, and executive leadership if log analysis confirms that any authenticated session accessed more than 50 distinct peer profiles via social-graph or DNA Relatives endpoints in a single session window, as this pattern confirms active data exfiltration of genetic PII triggering mandatory breach notification obligations under California CCPA/CPRA and potentially HIPAA if health-predisposition data is involved, and given the active California AG lawsuit any evidence of ongoing or uncontained exposure requires immediate outside counsel engagement.

Recovery Notes	After MFA enforcement, lockout configuration, and API-level data isolation are deployed, validate each control independently against a staging environment clone before restoring the DNA Relatives or social-graph features to full production availability. Maintain elevated logging verbosity (full request/response metadata, not just status codes) on all social-graph API endpoints for a minimum of 90 days post-remediation to capture any resumed campaign targeting newly registered or previously unaffected accounts. Given that credential stuffing relies on previously breached credential lists that remain in circulation indefinitely, the 30-day monitoring window should be extended to 90 days for accounts holding genetic health predisposition data, which carries substantially higher re-targeting risk than standard PII.
Forensic Artifacts	Web application authentication logs (nginx/Apache/IIS access logs or IdP audit logs): sequential records of HTTP 401 responses followed by HTTP 200 on the /login or /oauth/token endpoint from the same source IP or /24 subnet within short time windows — the direct signature of successful credential stuffing preceding the 23andMe data access | Application-layer API response logs for DNA Relatives or social-graph endpoints: records showing a single authenticated session token (JWT or session cookie) making API calls that return profile data belonging to user IDs other than the authenticated user — this cross-user data return pattern is the specific forensic artifact of the traversal exploit used in the 23andMe breach | Identity provider or database authentication records: rows in the users/sessions table showing last_login timestamps and source IP geolocation for the breach window, cross-referenced against the list of victim user IDs whose profiles appeared in API responses — required to establish which accounts were both compromised (attacker logged in as them) versus scraped (their data was returned to another session) | CDN or load balancer access logs (Cloudflare, AWS CloudFront, Fastly): these upstream logs capture the full distributed IP pool used in the credential stuffing campaign before application-layer logs rotate, and will show the user-agent strings (often mimicking legitimate browsers) and request timing patterns characteristic of automated stuffing tools such as Sentry MBA or SNIPR | Application database query logs or ORM audit trails: records of SELECT queries against the genetic profile, ancestry composition, or family relationship tables during the breach window, joinable to session identifiers — establishes the precise data fields exfiltrated and the enumerated victim population required for both regulatory notification scoping and the California AG's damages calculation

Per-Action IR Details

Containment — Audit all consumer-facing applications that expose social or network-graph features (e.g., 'connected accounts', 'people you know', 'data sharing' toggles). Immediately evaluate whether an authenticated user can traverse beyond their own data to scrape peer profiles. Disable or rate-limit any such feature until access controls are verified.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST AC-3 (Access Enforcement), NIST AC-4 (Information Flow Enforcement), NIST AC-6 (Least Privilege), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Using nginx or Apache, immediately inject a rate-limiting rule on the social-graph or data-sharing API endpoints: for nginx, add 'limit_req_zone $binary_remote_addr zone=dna_api:10m rate=10r/m;' in the server block. For a 2-person team without a WAF, run 'netstat -an | grep ESTABLISHED | awk "{print $5}" | cut -d: -f1 | sort | uniq -c | sort -rn | head -20' every 15 minutes to identify IPs generating abnormal session counts against the social-graph endpoints. Document all features touched before disabling so recovery is reversible.

Evidence: Before disabling any feature, capture application server access logs (e.g., /var/log/nginx/access.log or IIS logs in W3C format) showing authenticated session tokens (cookies/JWTs) making sequential GET requests to profile

or DNA Relatives endpoints across multiple distinct user IDs — this traversal pattern (one session, many victim UIDs) is the direct forensic signature of the 23andMe-style scrape. Also snapshot current API rate-limit configuration files and any feature-flag or toggle configuration to establish pre-remediation baseline.

Detection — Review authentication logs for high-volume login attempts against a single account or distributed low-volume attempts across many accounts (credential stuffing signature). In your SIEM, query for: multiple failed logins followed by success from the same IP or IP range; single accounts accessed from geographically anomalous locations in short windows; and abnormal API or feature call volumes on data-sharing or social-graph endpoints. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-3 (Content of Audit Records), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, run the following bash one-liner against your web application auth logs to surface credential stuffing patterns: 'awk \'$9=="401" || $9=="200" {print $1, $7, $9}\' /var/log/nginx/access.log | sort | uniq -c | sort -rn | head -50'. Cross-reference successful logins (HTTP 200 on /login or /oauth/token) that are preceded within 60 seconds by 5+ HTTP 401s from the same /24 subnet. For the DNA Relatives traversal detection, query: 'grep -E "(dna-relatives|profile-share|family-network)" /var/log/nginx/access.log | awk \'{print $1}\' | sort | uniq -c | sort -rn' to find sessions hitting those endpoints at anomalous frequency. Use the free Sigma rule 'Credential Stuffing - Multiple Failed Logins Followed By Success' (SigmaHQ repository) adapted to your log format.

Evidence: Preserve raw authentication logs (minimum 90 days) showing failed/success sequences with full timestamps, source IPs, user-agent strings, and authenticated user identifiers before any log rotation occurs. Capture application-layer logs showing which user profile IDs were returned in API responses during the anomalous session windows — in the 23andMe breach, the scrape of DNA Relatives data means the response payloads (not just requests) are forensically relevant. Also preserve any WAF or CDN logs (Cloudflare, AWS WAF) that may show the distributed IP pool used in the stuffing campaign before those external logs expire.

Eradication — Enforce account lockout or CAPTCHA challenges after a defined number of failed login attempts per NIST AC-7 (Unsuccessful Logon Attempts). Require multi-factor authentication on all consumer accounts per CIS 6.3 (Require MFA for Externally-Exposed Applications). Apply least-privilege data access to social or network features so authenticated users can only retrieve their own records per NIST AC-6 (Least Privilege) and NIST AC-3 (Access Enforcement).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-7 (Unsuccessful Logon Attempts), NIST AC-6 (Least Privilege), NIST AC-3 (Access Enforcement), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 5.2 (Use Unique Passwords)

Compensating: For teams without a commercial MFA platform, integrate Google Authenticator TOTP via the free 'speakeasy' Node.js library or 'pyotp' in Python into the login flow. For CAPTCHA without budget, deploy hCaptcha (free tier). For lockout enforcement without an identity provider, implement a Redis-backed counter: increment on each 401, trigger lockout flag at threshold 5 within 300 seconds, block further auth attempts for 900 seconds. For the data-access isolation specific to the DNA Relatives traversal vector, add a server-side assertion in the profile retrieval API handler that compares the authenticated session's user ID against the requested profile ID and returns HTTP 403 if they do not match — this directly closes the traversal path that enabled the 23andMe scrape.

Evidence: Before deploying lockout and MFA changes, extract from your identity store (LDAP, database, or IdP) the full list of accounts that authenticated successfully during the anomalous window identified in detection — these are confirmed-compromised accounts requiring forced password reset and session invalidation. Additionally, query your application database for any user accounts that were accessed via the DNA Relatives or social-graph API during the breach window but who did not themselves initiate a login session during that period (i.e., victim profiles scraped without their own login activity) — this enumeration defines your notification population.

Recovery — After tightening controls, verify remediation by running a controlled credential stuffing simulation (low-volume, authorized) against your authentication endpoints to confirm lockout thresholds trigger correctly. Monitor for resumed anomalous login patterns for at least 30 days. Validate that the DNA Relatives-style traversal pattern (authenticated user accessing peer profile data at scale) is no longer possible per NIST AC-4 (Information Flow Enforcement).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-4 (Information Flow Enforcement), NIST AC-7 (Unsuccessful Logon Attempts), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 7.3 (Perform Automated Operating System Patch Management)

Compensating: Use the open-source tool 'Hydra' (in an authorized, isolated test environment against a staging clone, never production) to simulate a low-volume credential stuffing run against the /login endpoint using a 50-credential test list — confirm that lockout fires at the configured threshold and that the blocked IP receives HTTP 429 or 403. For traversal validation, write a pytest or Postman collection test that authenticates as User A and attempts to retrieve User B's DNA Relatives profile data via direct API call; assert that the response returns HTTP 403 and contains zero records belonging to User B. Schedule this test to run weekly via cron against staging as a regression gate before any auth or social-graph code change is promoted to production.

Evidence: During the 30-day monitoring window, retain daily snapshots of the top-50 source IPs by authentication attempt volume and the top-50 user accounts by DNA Relatives or social-graph API call frequency — deviations from the post-remediation baseline are your early-warning signal for resumed campaign activity. Preserve all test artifacts from the authorized stuffing simulation (test credential list, timestamps, response codes, lockout confirmation logs) as evidence of control verification for regulatory or litigation purposes given the active California AG lawsuit.

Post-Incident — Conduct a formal review of data minimization and access control design for any feature that exposes user-to-user data relationships. Map findings to NIST AC-5 (Separation of Duties) and NIST AC-6 (Least Privilege). Review breach notification procedures against applicable state privacy laws. Document findings in your risk register and update your incident response playbook to include credential stuffing as an explicit scenario. Apply D3-MFA (Multi-factor Authentication) and D3-UAP (User Account Permissions) as standing countermeasures.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST AC-5 (Separation of Duties), NIST AC-6 (Least Privilege), NIST IR-4 (Incident Handling), NIST AU-11 (Audit Record Retention), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 3.2 (Establish and Maintain a Data Inventory)

Compensating: Use OWASP's free Threat Modeling tool (OWASP Threat Dragon) to document the DNA Relatives data-flow diagram and annotate trust boundaries where authenticated user scope must be enforced — this produces a repeatable artifact for future feature design reviews. For breach notification tracking against California CCPA/CPRA and other state laws, maintain a plain-text notification obligation matrix (state, trigger threshold, deadline, regulator contact) updated annually; the 23andMe case establishes that 855,000-person genetic data exposure without timely notification triggers AG enforcement, so the notification SLA must be explicit in your playbook. Archive all incident documentation (logs, timelines, notification records, remediation evidence) for a minimum of 5 years per NIST AU-11 (Audit Record Retention) given active litigation.

Evidence: Compile the complete incident timeline documenting: first evidence of credential stuffing attempts in auth logs, first evidence of DNA Relatives traversal API calls, date security team detected anomaly, date containment actions were taken, and date affected users were notified — this timeline is the primary document in California AG enforcement proceedings and must be reconstructed from preserved log evidence, not from memory. Additionally, produce a data inventory (per CIS 3.2) documenting exactly which data fields (name, ancestry composition, health predispositions, family relationships) were accessible via the traversal path and were therefore in scope of the exposure.

Detection Guidance

Detection centers on identifying credential stuffing patterns and abnormal data access volume on authenticated endpoints. Key signals: (1) Auth logs, clusters of failed logins from rotating IPs targeting many distinct accounts within a short window; low-and-slow distributed attempts may evade threshold alerts, so tune for cumulative failed attempts per account over longer windows (e.g., 10 failures in 24 hours), not just burst patterns. (2) Application logs, authenticated sessions making unusually high volumes of requests to social-graph, profile-sharing, or data-export endpoints; baseline normal per-session call volumes and alert on deviations exceeding 3x the 90-day average. (3) SIEM correlation rule, join auth success events with subsequent high-volume feature API calls within the same session; flag sessions where data retrieval volume exceeds individual-account norms. (4) User behavior analytics, flag accounts accessed from new device fingerprints or geolocation outliers immediately following a high-failure login period. Reference NIST SI-4 (System Monitoring) and NIST AU-6 for log review cadence. D3-LAM (Local Account Monitoring) applies to internal privileged account monitoring in parallel.

Framework Mappings

MITRE-ATTACK

- **T1110.004** — Credential Stuffing
- **T1078** — Valid Accounts
- **T1530** — Data from Cloud Storage

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-7** — Unsuccessful Logon Attempts

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(6)(ii)** — Response and Reporting

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures
- **CC7.4** — Responds to identified security incidents

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information
- **A.5.23** — Information security for use of cloud services

NIST-CSF-2

- **RS.CO-03** — Recovery activities and progress communicated

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1110.004	Credential Stuffing	Credential-Access
T1078	Valid Accounts	Defense-Evasion
T1530	Data from Cloud Storage	Collection

Sources

Source	URL	Tier
	https://oag.ca.gov/news/press-releases/attorney-general-bonta-sues-...	T1
California Attorney General to sue 23andMe over 2023 data breach	https://www.bbc.com/news/articles/crepleq2zyvo	T2
California sues 23andMe, alleging it failed to protect user data in ...	https://abcnews.com/Technology/wireStory/california-sues-23andme-al...	T3
Attorney - 23andMe failed to take basic steps to protect users' data ...	https://www.facebook.com/AGRobBonta/photos/23andme-failed-to-take-b.. .	T3
California suit says 23andMe hack exposed 855,000 Californians ...	https://krcrtv.com/news/local/california-suit-says-23andme-hack-exp...	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-05-30 06:23 UTC by TJS Security Command Center